# 日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年１１月２２日

出 願 番 号
Application Number: 特願２０００－３５５９６８

願 人
Applicant (s): ミノルタ株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 １月２６日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３０００７２２

【書類名】　特許願
【整理番号】　174604
【提出日】　平成12年11月22日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　9/00
【発明者】
【住所又は居所】　大阪府大阪市中央区安土町二丁目３番１３号大阪国際ビル　ミノルタ株式会社内
【氏名】　正木　賢治
【特許出願人】
【識別番号】　000006079
【住所又は居所】　大阪府大阪市中央区安土町二丁目３番１３号大阪国際ビル
【氏名又は名称】　ミノルタ株式会社
【代理人】
【識別番号】　100062144
【弁理士】
【氏名又は名称】　青山　葆
【選任した代理人】
【識別番号】　100086405
【弁理士】
【氏名又は名称】　河宮　治
【先の出願に基づく優先権主張】
【出願番号】　特願2000-　73
【出願日】　平成12年 1月 4日
【手数料の表示】
【予納台帳番号】　013262
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9808001

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　出力システム及びそれに用いる出力方法並びに出力システムにおいて実行されるプログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】　データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、

上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、

上記データ処理装置から出力装置へのデータ送信に際し、上記ドライバソフトウェアを経由する出力要求であるか否かを判断する判断手段と、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止する禁止手段とを有していることを特徴とする出力システム。

【請求項２】　データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、

上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、

上記データ処理装置側で、上記ドライバソフトウェアを経由するデータを暗号化する暗号化手段と、

上記出力装置側で、上記暗号化手段により暗号化されたデータを解読する解読手段とを有していることを特徴とする出力システム。

【請求項３】　データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、

上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、

上記データ処理装置から出力装置へのデータ出力要求に対して、上記出力装置へデータを出力するための設定値とは異なる設定値を設定することにより、上記出力装置へのデータ出力を禁止する禁止手段を有していることを特徴とする出力システム。

【請求項４】　上記設定値は、所定のレジスタに格納される値であることを

特徴とする請求項３記載の出力システム。

【請求項５】　データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、

上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断した上で、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止することを特徴とする出力方法。

【請求項６】　データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、

上記データ処理装置側で、該データ処理装置に組み込まれたドライバソフトウェアを経由するデータを暗号化し、

上記出力装置側で、暗号化されたデータを解読するステップを有していることを特徴とする出力方法。

【請求項７】　データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて実行されるプログラムを記録した記録媒体であって、該プログラムが、

上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断するステップと、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するステップとを有していることを特徴とするコンピュータ読取り可能な記録媒体。

【請求項８】　データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置において実行されるプログラムを記録した記録媒体であって、該プログラムが、

アプリケーションプログラムから出力される出力データに対して所定の暗号化処理を行なうステップと、

上記暗号化ステップにより暗号化された出力データを上記出力装置に対して出

力するステップとを有していることを特徴とするコンピュータ読取り可能な記録媒体。

【請求項９】　上記暗号化処理ステップは、アプリケーションプログラムから出力される出力データに対して、所定のパスワードを設定するステップであることを特徴とする請求項８記載のコンピュータ読取り可能な記録媒体。

【請求項１０】　データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置に、上記出力装置を使用可能にするためのドライバソフトウェアをインストールするインストールプログラムを記録した記録媒体であって、該インストールプログラムが、

上記データ処理装置にドライバソフトウェアをインストールするステップと、

上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するプログラムをインストールするステップとを有していることを特徴とするコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、プリント又はコピーを出力するための出力システムに関する。

【０００２】

【従来の技術】

近年、カラー複写機，カラープリンタ若しくはカラースキャナなどの性能向上及び低価格化が進むにつれ、不正なプリント又はコピー（例えば紙幣，有価証券若しくは金券のプリント又はコピー）が容易に行える環境になりつつある。

【０００３】

図１１に、従来の典型的な出力システムにおけるデータの流れを示す。この出力システムは、基本ソフトウェアであるオペレーティングシステム(以下、ＯＳという)５２及び該ＯＳ５２からの制御データに基づいて動作するハードウェア５５を含むコンピュータ５０と、該コンピュータ５０に接続されたプリンタ６０とから構成される。上記コンピュータ５０では、ＯＳ５２により、例えば画面の表示や文書の保存などの各種の機能が提供されるようになっている。このＯＳ５

２は、その中核部分であるカーネルとは切り離してプリンタを制御し得るプリンタドライバソフトウェア(以下、プリンタドライバという)５３を有しており、また、ＯＳ５２の一部には、アプリケーションプログラム（図中のアプリケーションＡ及びＢ）の各種要求に応じて、ＯＳ５２上の各種機能を呼び出す仕様としてのＡＰＩ(Application Programming Interface)５４が設定されている。

【０００４】

一般に、汎用のＯＳが組み込まれたコンピュータを含む出力システムにおいて印刷が行われる場合には、アプリケーションプログラムからのプリント要求に応じて、プリンタドライバ５３及びＡＰＩ５４を順次呼び出し、プリンタドライバ５３上でデータを作成した上で、ハードウェア５５のプリンタＩ／Ｏ５６へ送信する方法(図中、アプリケーションＡからの経路)、及び、プリンタドライバ５３上でデータを作成することなく、アプリケーションプログラムからＡＰＩ５４を介してハードウェア５５のプリンタＩ／Ｏ５６へ直接に送信される方法(図中、アプリケーションＢからの経路)の２通りの方法が実施可能である。

【０００５】

【発明が解決しようとする課題】

ところで、従来、かかる出力システムにおいて、不正なプリント又はコピーを防止するには、プリンタドライバ５３に不正プリント／コピー防止機能をもたせることが一般的である。しかし、前述したような出力システムでは、例えば、プリント対象であるデータをコンピュータ５０側で圧縮し、プリンタ６０側で伸張する処理を行なう場合など、コンピュータ５０から出力されるデータを取り出して解析することにより、プリンタ６０での処理内容を解読する場合には、プリンタドライバ５３を迂回して、すなわち、プリンタドライバ５３上でデータを作成することなく、プリンタ６０へアクセスすることが可能となっており、この経路では、不正プリント／コピーを防止することができない。

【０００６】

なお、現在、カラー複写機については、不正プリント／コピー防止用手段の装備が義務付けられているが、このような付加的な手段は、一般的に、ハードウェアとして実装されるため、機器のコスト増大を回避し得ない。

また、例えばＬＡＮ等の、複数台のコンピュータ及び該コンピュータに接続される複数台のプリンタから構成されるシステムにおいては、プリンタ側に不正プリント／コピー防止用装置を設置する場合、個々のプリンタが同様の不正プリント／コピー防止用装置をもつことになり、無駄が生じる。

【０００７】

そこで、本発明は、上記技術的課題に鑑みてなされたもので、安価且つ安全な出力システム及びそれに用いる出力方法並びに出力システムにおいて実行されるプログラムを記録した記録媒体を提供することを目的とする。

【０００８】

【課題を解決するための手段】

本願の請求項１に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ送信に際し、上記ドライバソフトウェアを経由する出力要求であるか否かを判断する判断手段と、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止する禁止手段とを有していることを特徴としたものである。

【０００９】

また、本願の請求項２に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置側で、上記ドライバソフトウェアを経由するデータを暗号化する暗号化手段と、上記出力装置側で、上記暗号化手段により暗号化されたデータを解読する解読手段とを有していることを特徴としたものである。

【００１０】

更に、本願の請求項３に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得る不正プリント防止

機能を備えたドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ出力要求に対して、上記出力装置へデータを出力するための設定値とは異なる設定値を設定することにより、上記出力装置へのデータ出力を禁止する禁止手段を有していることを特徴としたものである。

【００１１】

また、更に、本願の請求項４に係る発明は、請求項３に係る発明において、上記設定値が、所定のレジスタに記憶される値であることを特徴としたものである。

【００１２】

また、更に、本願の請求項５に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断した上で、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止することを特徴としたものである。

【００１３】

また、更に、本願の請求項６に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、上記データ処理装置側で、該データ処理装置に組み込まれたドライバソフトウェアを経由するデータを暗号化し、上記出力装置側で、暗号化されたデータを解読するステップを有していることを特徴としたものである。

【００１４】

また、更に、本願の請求項７に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて実行されるプログラムを記録した記録媒体であって、該プログラムが、上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する

出力要求であるか否かを判断するステップと、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するステップとを有していることを特徴としたものである。

【００１５】

また、更に、本願の請求項８に係る発明は、データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置において実行されるプログラムを記録した記録媒体であって、該プログラムが、アプリケーションプログラムから出力される出力データに対して所定の暗号化処理を行なうステップと、上記暗号化ステップにより暗号化された出力データを上記出力装置に対して出力するステップとを有していることを特徴としたものである。

【００１６】

また、更に、本願の請求項９に係る発明は、請求項８に係る発明において、上記暗号化処理ステップが、アプリケーションプログラムから出力される出力データに対して、所定のパスワードを設定するステップであることを特徴としたものである。

【００１７】

また、更に、本願の請求項１０に係る発明は、データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置に、上記出力装置を使用可能にするためのドライバソフトウェアをインストールするインストールプログラムを記録した記録媒体であって、該インストールプログラムが、上記データ処理装置にドライバソフトウェアをインストールするステップと、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するプログラムをインストールするステップとを有していることを特徴としたものである。

【００１８】

【発明の実施の形態】

以下、本発明の実施の形態について、添付図面を参照しながら説明する。

実施の形態１．

図１は、本発明の実施の形態１に係る出力システムを含むネットワークを示す

説明図である。このネットワーク１００は、ネットワーク全体の制御，管理等および他のネットワーク構成から要求されるファイル検索などの仕事を実行するサーバコンピュータ１２と、複数台のクライアントコンピュータ１０と、該クライアントコンピュータ１０から送信されてきたデータを印字プリントとして出力するプリンタ２０とを有している。上記サーバコンピュータ１２には、各種のデータを系統的に管理するデータベース１２Ａが付属させられ、該データベース１２Ａは、必要に応じて、各クライアントコンピュータ１０からアクセスされ、データの書込み又は読出しが行われる。

【００１９】

各クライアントコンピュータ１０は、基本ソフトウェアであるオペレーティングシステム(以下、ＯＳという)２及び該ＯＳ２の制御データに基づいて動作するハードウェア５（ＯＳ２及びハードウェア５ともに図２参照）を含んでおり、ネットワーク１００がインターネット１９に接続されていることから、これらクライアントコンピュータ１０では、例えば電子メールやＦＴＰ（File Transfer Protcol）によるファイル転送，WWWによるホームページ閲覧，該ホームページからの各種形式データのダウンロード等のサービスが利用可能である。ここでは、クライアントコンピュータ１０に組み込まれるＯＳ２として、ウィンドウズ（Windows）が採用されている。なお、これに限定されることなく、例えばユニックス(UNIX)若しくはＭＳ－ＤＯＳ等の汎用ＯＳを採用してもよい。

【００２０】

本実施の形態に係る出力システムは、クライアントコンピュータ１０からプリンタ２０へデータ送信するに際して、不正なプリント又はコピーを防止すべく、不正なジョブデータについては、その送信を禁止する若しくはプリンタ２０側での出力を禁止することを可能とする、クライアントコンピュータ１０とそれに接続されたプリンタ２０とから構成される出力システムである。以下、この出力システムについて説明する。なお、以下の説明では、クライアントコンピュータ１０を単にコンピュータ１０という。

【００２１】

図２は、コンピュータ１０とプリンタ２０とから構成される出力システムの構

成を示す説明図である。コンピュータ１０では、ＯＳ２により例えば画面の表示や文書の保存などの各種の機能が提供されるようになっており、ＯＳ２が、その中核部分であるカーネルとは切り離して所定のハードウェアを制御し得るソフトウェア形態のデバイスドライバを複数有しており、これらデバイスドライバの１つとして、プリンタ２０を制御し得るプリンタドライバ３がインストールされている。プリンタドライバ３は、一般的に、プリンタ本体販売時に同梱されているＣＤ－ＲＯＭ１５又はフロッピーディスク１６等の外部記録媒体より、コンピュータ１０にインストールされる。通常、このプリンタドライバ３のインストールに際して、プリンタドライバ３のインストールをユーザの目的に応じて半自動又は自動的に行なえるようにするためのプログラムであるインストーラが用意されており、このインストーラプログラムが、ＣＤ－ＲＯＭ１５又はフロッピーディスク１６等の外部記録媒体より、コンピュータ１０にプリンタドライバをインストールする。

【００２２】

また、ＯＳ２の一部には、アプリケーションプログラム(図中のアプリケーションＡ及びＢ)のプリント要求に応じて、ＯＳ２上のプリント機能を呼び出す仕様としてのＡＰＩ４（図中では「Ｍｏｄｉｆｉｅｄ ＡＰＩ」と表記）が設定されている。この実施の形態１において、ＡＰＩ４は、ＯＳ２上に予め設定されていたＡＰＩ、すなわち、アプリケーションプログラムからプリンタへの直接的なアクセスを可能とするＡＰＩ（従来例を示す図１１参照）が置き換えられてなるもので、詳しくは図３のフローチャートを参照して後述するが、このＡＰＩ４は、プリンタドライバ３を迂回してきたデータについて、プリンタ２０へのデータ送信機能を無効とし、これにより、データがＡＰＩ３を介してプリンタ２０へ直接に送られることを禁止し得る。

【００２３】

ＡＰＩ４は、前述したプリンタドライバ３のインストール時に、ＣＤ－ＲＯＭ１５又はフロッピーディスク１６より、コンピュータ１０にインストールされる。このインストールに際して、ＯＳ２上に存在していたオリジナルのＡＰＩは、上書きされてディスク上に存在しなくなるか、若しくは、バックアップファイル

として別名に書き換えられる。これにより、図２に示すＯＳ２では、アプリケーションＡ及びＢからのプリント要求に応じて、常時、新たにインストールされたＡＰＩ４が呼び出されるようになっている。

ＯＳ２として、例えばウィンドウズ（Ｗｉｎｄｏｗｓ）を採用する場合、ＡＰＩはＤＬＬファイルとして提供される。ＡＰＩ４のインストールにより、オリジナルのＤＬＬファイルは、新たにインストールされるＤＬＬファイルに置き換えられる。

【００２４】

以上の構成を備えたＯＳ２では、通常、アプリケーションＡ及びＢからのプリント要求に応じて、まず、プリンタドライバ３が、アプリケーションプログラムからのプリント要求に応じて呼び出され、続いて、ＡＰＩ４が呼び出される。そして、データがプリンタドライバ３を経由するものであるか否かを判断し、プリンタドライバ３を経由する場合には、プリンタドライバ３上でのデータ作成処理が行なわれる。その後、データは、ハードウェア５に組み込まれたプリンタＩ／Ｏ６へ入力され、プリンタ２０への送信に適した形式に変換された上で送信される。

【００２５】

このプリンタドライバ３では、従来知られるように、プリント対象であるデータを作成するに際して、不正なプリントの防止を可能とし、不正なジョブデータを受けた場合、そのデータについては、プリンタ２０へのアクセスを拒否することができる。このように、プリンタドライバ３を経由した場合には、不正なデータがプリンタ２０へのアクセスを拒否されるようになっており、不正プリントの防止が実現される。

【００２６】

また、一方、データがプリンタドライバ３を経由しない場合、すなわち、データがプリンタドライバ３を迂回する場合、この実施の形態１では、ＯＳ２において、ＡＰＩ４のファンクションコール（以下、ＡＰＩコールという）がトラップされて独自のルーチンに置きかえられることで、プリンタへのデータ送信機能が無効にされ、これにより、一切のデータがＡＰＩ４を介してプリンタ２０へ直接

に送られることが禁止される。その結果、不正なデータは、プリンタ８へのアクセスを拒否され、不正プリントの防止が実現される。

【００２７】

図３は、出力システムにおける不正プリント防止動作についてのフローチャートである。まず、＃１１では、アプリケーションプログラムからのプリント要求に応じて、プリンタドライバ３を呼び出し、続いて、＃１２では、ＡＰＩ４を呼び出す。＃１３では、プリント要求をあらわすＡＰＩコールをトラップする。そして、＃１４では、ＡＰＩコールに基づき、プリンタドライバ３の経由が要求されているか否かを判断する。その結果、プリンタドライバ４の経由が要求されない場合には、＃１５へ進み、プリンタ２０への直接アクセスを禁止して、処理を終了する。他方、プリンタドライバ４の経由が要求される場合、＃１６へ進む。

【００２８】

＃１６では、プリンタドライバ３に予め組みこまれている不正プリント防止機能を呼び出す。続いて、＃１７では、不正プリントであるか否か、すなわち、プリント対象であるデータが不正なデータであるか否かを判断する。その結果、不正プリントである場合には、＃１８へ進み、プリンタ２０へのアクセスを拒否して、処理を終了する。他方、不正なプリントではない場合には、＃１９へ進み、プリンタ２０へアクセスする。その後、＃２０では、プリンタ２０にて、データに基づき印刷を行ない、プリントを出力する。

【００２９】

このようにして、上記出力システムでは、プリンタドライバ３を経由する場合および迂回する場合共に、不正なプリントを防止することができる。かかる不正プリント防止動作は、コンピュータ１０に組み込まれたＯＳ２のプログラムに基づいて実行されるものであり、この実施の形態１では、該プログラムが、コンピュータ１０内のハードディスクにインストールされており、メモリ上に呼び出されて実行される。なお、これに限定されることなく、このようなプログラムは、例えばフロッピーディスク，ＣＤ－ＲＯＭ等の外部記録媒体にファイル形式で保存され、そこから呼び出すようにしてもよい。

【００３０】

以上のように、この実施の形態１では、ハードウェア面での追加投資なしに、ソフトウェア面における補充を行うのみにより、安価で且つ信頼性の高い不正プリントの防止が可能な出力システムを実現することができる。また、この場合には、プリンタドライバ４に不正プリントの防止技術が搭載されるため、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【００３１】

なお、この実施の形態１では、プリンタドライバ３，そのインストーラ，ＡＰＩ４が、ＣＤ－ＲＯＭ１５又はフロッピーディスク１６等の外部記録媒体より、コンピュータ１０にインストールされるが、これに限定されることなく、コンピュータ１０に接続されたＬＡＮやネットワークを介して、他のコンピュータからドライバソフトウェアをダウンロード及びインストールするようにしてもよい。

【００３２】

また、図４には、インストーラによるプリンタドライバ３及びＡＰＩ４のインストール動作についてのフローチャートを示す。このインストール動作では、コンピュータ１０にプリンタドライバ３をインストールし（＃２１）、続いて、ＡＰＩ４をインストールする（＃２２）。＃２１及び＃２２のステップは、これに限定されることなく、順序を入れ替えられても若しくは並行して行なわれてもよい。

【００３３】

実施の形態２．

図５は、本発明の実施の形態２に係る出力システムの構成を示す説明図である。この出力システムは、前述した実施の形態１における場合と同様に、基本ソフトウェアであるＯＳ３２及びその制御データに基づいて動作するハードウェア３５を含むコンピュータ３０と、該コンピュータ３１に接続されたプリンタ４０とから構成される。ＯＳ３２は、ソフトウェア形態のデバイスドライバの１つとして、プリンタ４０を制御し得るプリンタドライバ３３を有している。また、ＯＳ３２の一部には、アプリケーションプログラム(図中のアプリケーションＡ及びＢ)のプリント要求に応じてＯＳ３２上のプリント機能を呼び出す仕様としての

ＡＰＩ３４が設定されている。

【００３４】

プリンタドライバ３３は、プリント対象であるデータを作成するに際して、不正なプリントの防止を可能とし、不正なデータを受けた場合、そのデータについては、プリンタ４０へのアクセスを拒否することができる。更に、この実施の形態２では、プリンタドライバ３３は、正常プリントを行なう場合、すなわち、そのプリント出力が許可される正常データを受けた場合に、データの先頭にある１０バイト分のデータを反転させる暗号化機能を有している。

かかるプリンタドライバ３３を経由したデータ若しくは迂回したデータは、ハードウェア３５に組み込まれたプリンタＩ／Ｏ３６へ入力され、プリンタ４０への送信に適した形式に変換された上で、プリンタ４０へ送信される。

【００３５】

この実施の形態２では、プリンタドライバ３３におけるデータ反転の暗号化機能に対応して、プリンタ４０に組み込まれた制御部４１が、コンピュータ３０より送られてきたデータの先頭にある１０バイト分のデータを反転させる復号化機能（データ反転機能）を有しており、プリンタ４０は、この機能によるデータ反転後に、正常なデータについて出力を続行し、異常なデータについては出力を中止する動作を行う。ここで、「正常なデータ」とは、コンピュータ３０側で暗号化されたデータが、プリンタ４０側で再度反転されて元の形に戻ったデータをあらわし、他方、「異常なデータ」とは、プリンタドライバ３３を迂回して送信されてきたデータが、プリンタ４０側で反転されてなるデータをあらわす。

【００３６】

これにより、この実施の形態２に係る出力システムでは、不正なデータについて、それがプリンタドライバ３３を経由する場合、その不正プリント防止機能により、出力が防止され、他方、それがプリンタドライバ３３を迂回する場合には、プリンタ４０の制御部４１において設定された復号化機能を用いて、先頭にある１０バイト分のデータが反転させられたデータが異常データとみなすことにより、不正なプリントが防止される。

【００３７】

図６は、この出力システムにおける不正プリント防止動作についてのフローチャートである。まず、＃３１では、アプリケーションプログラムからのプリント要求に応じて、プリンタドライバ３３を呼び出し、続いて、＃３２では、ＡＰＩ３４を呼び出す。＃３３では、プリント要求をあらわすＡＰＩコールをトラップする。そして、＃３４では、ＡＰＩコールに基づき、プリンタドライバ３３の経由が要求されているか否かを判断する。その結果、プリンタドライバ４の経由が要求されない場合には、＃３５へ進み、他方、プリンタドライバ４の経由が要求される場合、＃３８へ進む。

【００３８】

＃３５では、プリンタ４０へ直接にアクセスする。続いて、＃３６では、プリンタ４０にて、データの先頭を１０バイト反転させる。＃３７では、データが異常データとみなされることから出力を中止し、処理を終了する。

【００３９】

＃３８では、プリンタドライバ３３に予め設定されている不正プリント防止機能を呼び出す。次に、＃３９では、不正プリントであるか否か、すなわち、プリント対象であるデータが不正なデータであるか否かを判断する。その結果、不正プリントである場合には、＃４０へ進み、プリンタ４０へのアクセスを拒否して、処理を終了する。他方、不正なプリントではない場合には、＃４１へ進み、データの先頭を１０バイト反転させ、＃４２では、プリンタ４０へアクセスする。

【００４０】

続いて、＃４３では、プリンタ４０にて、データの先頭を１０バイト反転させる。これにより、プリンタドライバ３３上でその先頭１０バイトが反転させられた反転させられたデータが、元の正常なデータに戻る。そして、＃４４では、データに基づき印刷を行ない、プリントを出力する。

このようにして、上記出力システムは、プリンタドライバ３３を経由する場合および迂回する場合共に、不正なプリントを防止することができる。

【００４１】

なお、前述した実施の形態２では、このような不正プリント防止機能を実現する手段としてのデータ暗号化手段が、プリンタドライバ３３を経由するデータの

先頭１０バイトを反転することによるものであったが、これに限定されることなく、かかる暗号化としては、例えばプリンタドライバ３３を経由するデータに、パスワードを付すようにしてもよい。この場合には、データ解読を行なうべく、プリンタ４０側に、上記パスワードを認識しデータを識別するプログラムを設ける必要がある。

【００４２】

以上のように、この実施の形態２では、ハードウェア面での追加投資なしに、ソフトウェア面における補充を行うのみにより、信頼性の高い不正プリントの防止が可能で、安価なシステムを実現することができる。また、この場合には、プリンタドライバ３３に不正プリントの防止技術が搭載されるため、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を比較的簡単に実施することができる。

また、この実施の形態２では、プリンタ４０のファームウェアに上記復号化プログラムを組み込むことにより、不正プリントの防止を実現するため、コストの増大が回避されるとともに、比較的高い安全性が確保される。

【００４３】

実施の形態３．

図７～１０を参照して、コンピュータに組み込まれるＯＳとして、ＭＳ－ＤＯＳを採用した場合について説明する。図７は、ＭＳ－ＤＯＳシステムにおけるプリント出力時のデータの流れを概略的に示す説明図である。このＭＳ－ＤＯＳシステムでは、アプリケーションプログラム（図中の「アプリケーション」）からのプリント要求に応じて発せられたプリントの命令に対し、所定のレジスタ（ＡＨ，ＡＬ，ＤＸレジスタ）に設定する内容として、通常プリント時に設定される値とは異なる値が設定されるように、システムを変更することにより、実質的には異なるレジスタを使用することになる。これによって、プリンタへのデータ送信を禁止して、通常のプリント動作を一切禁止することができる。

【００４４】

図８を参照してＭＳ－ＤＯＳシステムにて一般的に行なわれるデータ処理について説明する。ＭＳ－ＤＯＳシステムでは、システム起動時にＢＩＯＳ割込みテ

ーブルがセットされる。アプリケーションからのプリント要求に応じ、プリント対象とされるデータを、ＢＩＯＳ割込み呼出しの形でプリンタへ送信する。このとき、アプリケーションが文字Ａをプリントする場合に、ＡＨレジスタに０をセットし（＃５１）、文字Ａに相当するデータ６５をＡＬレジスタに格納し（＃５２）、ＤＸレジスタに、出力先のプリンタ番号を指定して（＃５３）、割込み命令としてのＩＮＴ１７命令を発する。

【００４５】

ＩＮＴ１７命令を受けたＣＰＵは、１７番に相当するアドレス（例えば「０００：００５ｃ」のアドレスから始まる４バイトに格納されているデータ）を割込みテーブルから取得する（＃５４）。その後、ＣＰＵは、スタックフレームを作成して該フレーム内にレジスタを退避させたのち（＃５５）、そのアドレスにジャンプして、割込みを行う（＃５６）。ジャンプした場所が、本来のプリンタコントロールを行なう場所であることにより、データがプリンタへ送信された後に、リターン命令が発せられると、制御又はアプリケーションに戻る。

【００４６】

図９は、本発明の実施の形態３に係るトラップ処理についてのフローチャートである。システム起動時に、自動起動されるトラッププログラムにて、ＢＩＯＳ割込みテーブルの「００００：００５ｃ」のアドレスから始まる４バイトの内容を、トラッププログラム内にコピーする（＃６１）。続いて、トラッププログラム内の擬似プリントルーチンのアドレスを「００００：００５ｃ」から始まる４バイトにコピーし（＃６２）、プログラムをメモリ上に残したまま終了する。

【００４７】

次に、図１０は、擬似プリントルーチンの動作についてのフローチャートである。擬似プリントルーチンでは、ＣＨレジスタの内容をＡＨレジスタにコピーし（＃７１）、ＣＬレジスタの内容をＡＬレジスタにコピーし（＃７２）、また、ＢＸレジスタの内容をＤＸレジスタにコピーする（＃７３）。そして、プリントルーチンアドレスを読み込み（＃７４）、トラッププログラム内にコピーした本体のプリントルーチンのアドレスにジャンプする（＃７５）。これにより、アプリケーションから見れば、プリントの命令が、ＡＨ，ＡＬ，ＤＸレジスタを使う

ものから、ＣＨ，ＣＬ，ＢＸレジスタを用いるものに変更されることになり、通常のプリント動作が一切行なえなくなる。

更に、この擬似プリントルーチンは、プリンタコントロールＩＣのポートを監視しており、データを送信していないにもかかわらず、ビジー信号が生じる場合には、異常対策として、プリンタＩＣ初期化命令を送る。

【００４８】

このようにして、本プリンタドライバは、最初からＣＨ，ＣＬ，ＢＸレジスタを使用するものであるため、本プリンタドライバを使うアプリケーションのみについて印刷を行なうことが可能となる。また、ＢＩＯＳを介さずに、データをプリンタコントロールＩＣへ直接に送信した場合にも、ＩＣがリセットされるため、不正な使用が防止される。

【００４９】

なお、本発明は、例示された実施の形態に限定されるものでなく、本発明の要旨を逸脱しない範囲において、種々の改良及び設計上の変更が可能であることは言うまでもない。

【００５０】

【発明の効果】

本願の請求項１に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ送信に際し、上記ドライバソフトウェアを経由する出力要求であるか否かを判断する判断手段と、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止する禁止手段とを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。

【００５１】

また、本願の請求項２に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置側で、上記ドライバソフトウェアを経由するデータを暗号化する暗号化手段と、上記出力装置側で、上記暗号化手段により暗号化されたデータを解読する解読手段とを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【００５２】

更に、本願の請求項３に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得る不正プリント防止機能を備えたドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ出力要求に対して、上記出力装置へデータを出力するための設定値とは異なる設定値を設定することにより、上記出力装置へのデータ出力を禁止する禁止手段を有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【００５３】

また、更に、本願の請求項４に係る発明は、上記設定値が、所定のレジスタに格納される値であるため、信頼性の高い不正プリントの防止が可能で、安全な出

力システムを実現することができる。

【００５４】

また、更に、本願の請求項５に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断した上で、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。

【００５５】

また、更に、本願の請求項６に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、上記データ処理装置側で、該データ処理装置に組み込まれたドライバソフトウェアを経由するデータを暗号化し、上記出力装置側で、暗号化されたデータを解読するステップを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【００５６】

また、更に、本願の請求項７に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて実行されるプログラムを記録した記録媒体であって、該プログラムが、上記データ処理装置から出力装置へのデータ送信に際し、該データ

処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断するステップと、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するステップとを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【００５７】

また、更に、本願の請求項８に係る発明によれば、データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置において実行されるプログラムを記録した記録媒体であって、該プログラムが、アプリケーションプログラムから出力される出力データに対して所定の暗号化処理を行なうステップと、上記暗号化ステップにより暗号化された出力データを上記出力装置に対して出力するステップとを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【００５８】

また、更に、本願の請求項９に係る発明によれば、上記暗号化処理ステップが、アプリケーションプログラムから出力される出力データに対して、所定のパスワードを設定するステップであり、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。

【００５９】

また、更に、本願の請求項１０に係る発明によれば、データを所定の形式で出

力する出力装置に対してデータを出力するデータ処理装置に、上記出力装置を使用可能にするためのドライバソフトウェアをインストールするインストールプログラムを記録した記録媒体であって、該インストールプログラムが、上記データ処理装置にドライバソフトウェアをインストールするステップと、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するプログラムをインストールするステップとを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１に係る出力システムが組み込まれたネットワークシステムを示す図である。

【図２】　上記出力システムの構成を示す説明図である。

【図３】　上記出力システムによる不正プリント防止動作のフローチャートである。

【図４】　インストーラによるプリンタドライバ及びＡＰＩのインストール動作のフローチャートである。

【図５】　本発明の実施の形態２に係る出力システムの構成を示す説明図である。

【図６】　上記実施の形態２に係る出力システムによる不正プリント防止動作のフローチャートである。

【図７】　本発明の実施の形態３に係るＭＳ－ＤＯＳシステムを採用した場合におけるデータの流れを概略的にします説明図である。

【図８】　ＭＳ－ＤＯＳシステムにて一般的に行なわれるデータ処理のフローチャートである。

【図９】　上記実施の形態３に係るトラップ処理のフローチャートである。

【図１０】　上記実施の形態３に係る疑似プリントルーチンである。

【図１１】　従来の出力システムの構成の一例を示す説明図である。

【符号の説明】

１０，３０…コンピュータ

２，３２…オペレーティングシステム

３，３３…プリンタドライバ

４，３４…ＡＰＩ

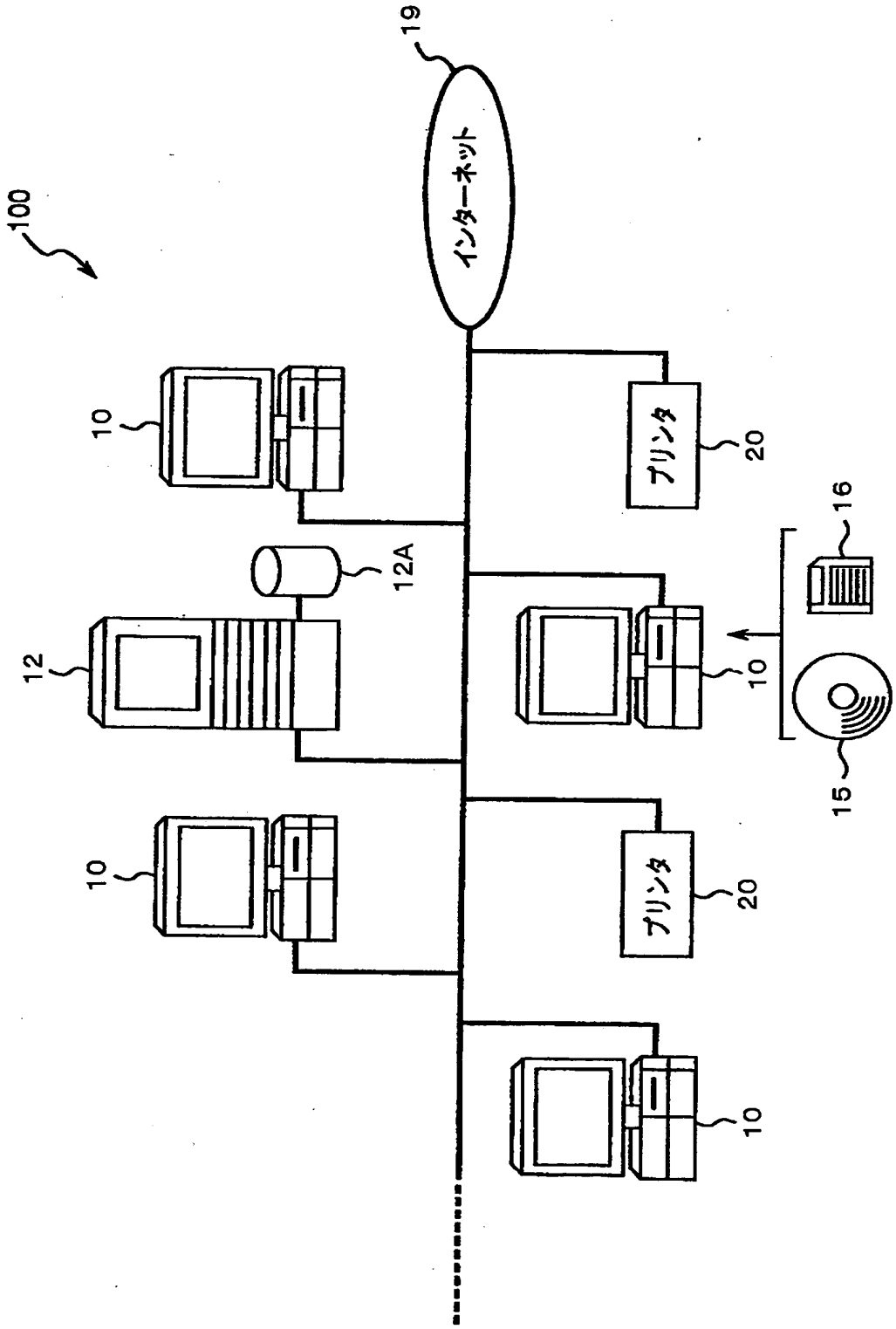
２０，４０…プリンタ

４１…プリンタ制御部

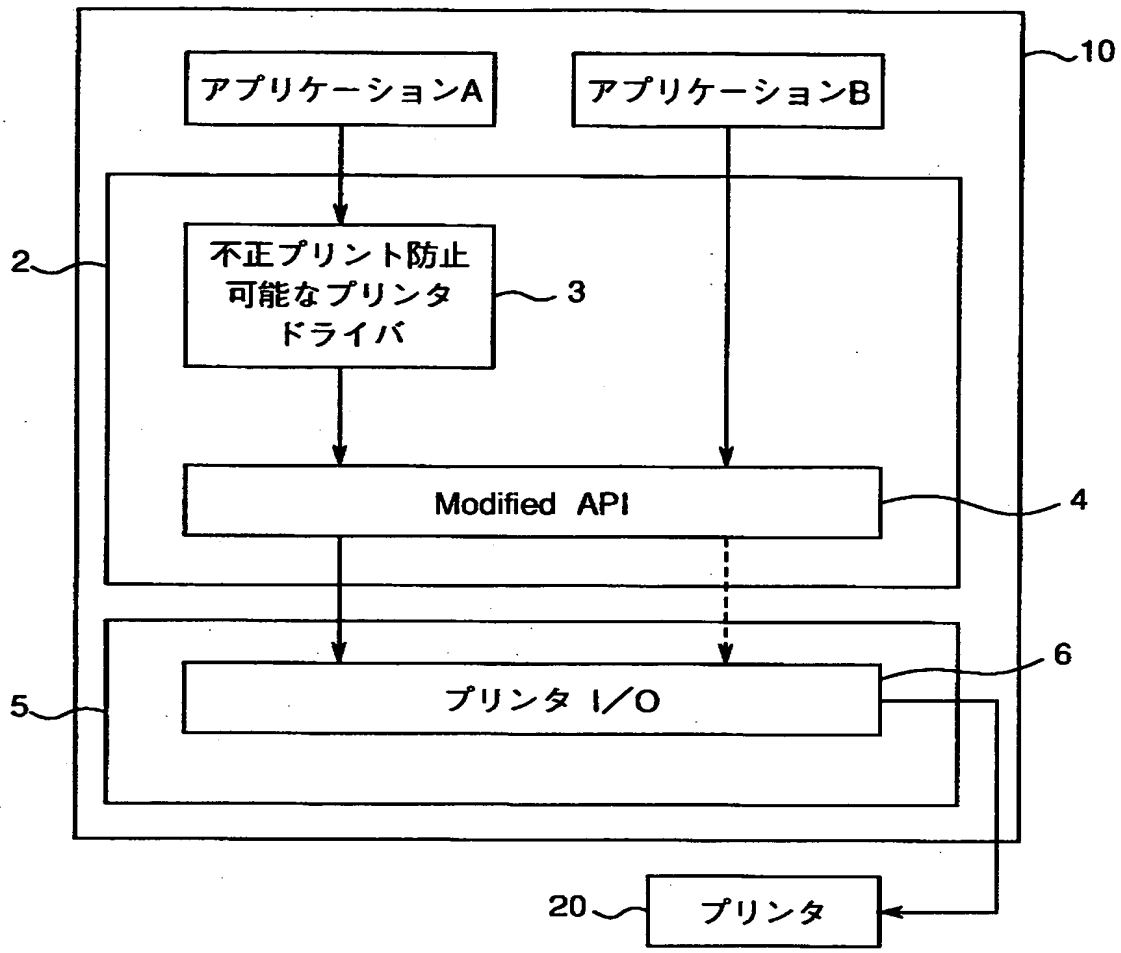
１００…ネットワーク

【書類名】　図面

【図１】



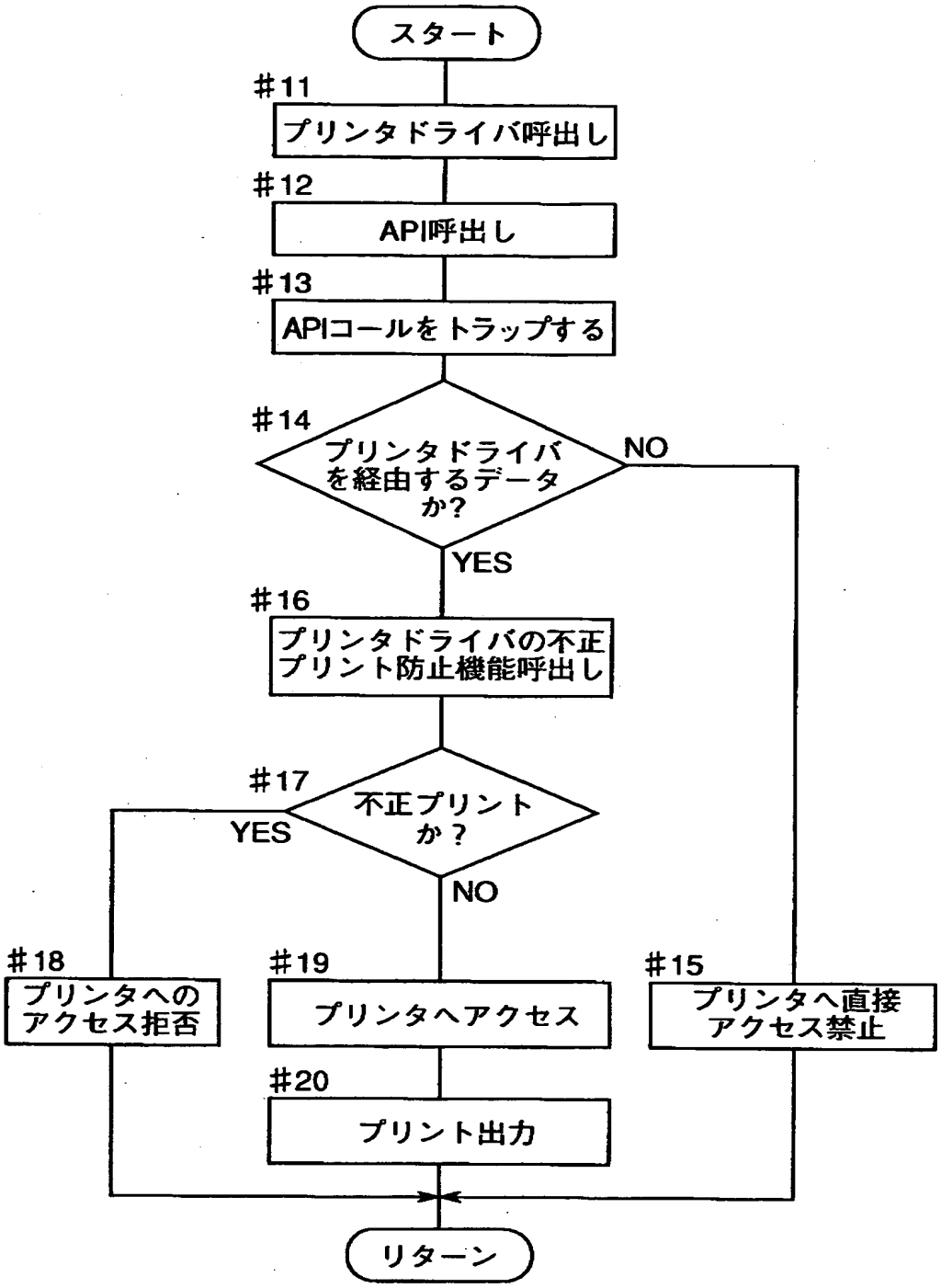
【図２】



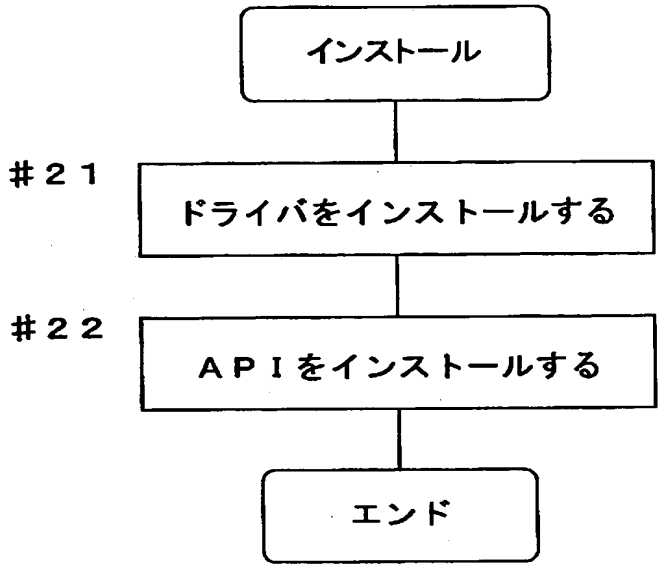



出証特２００１－３０００７２２

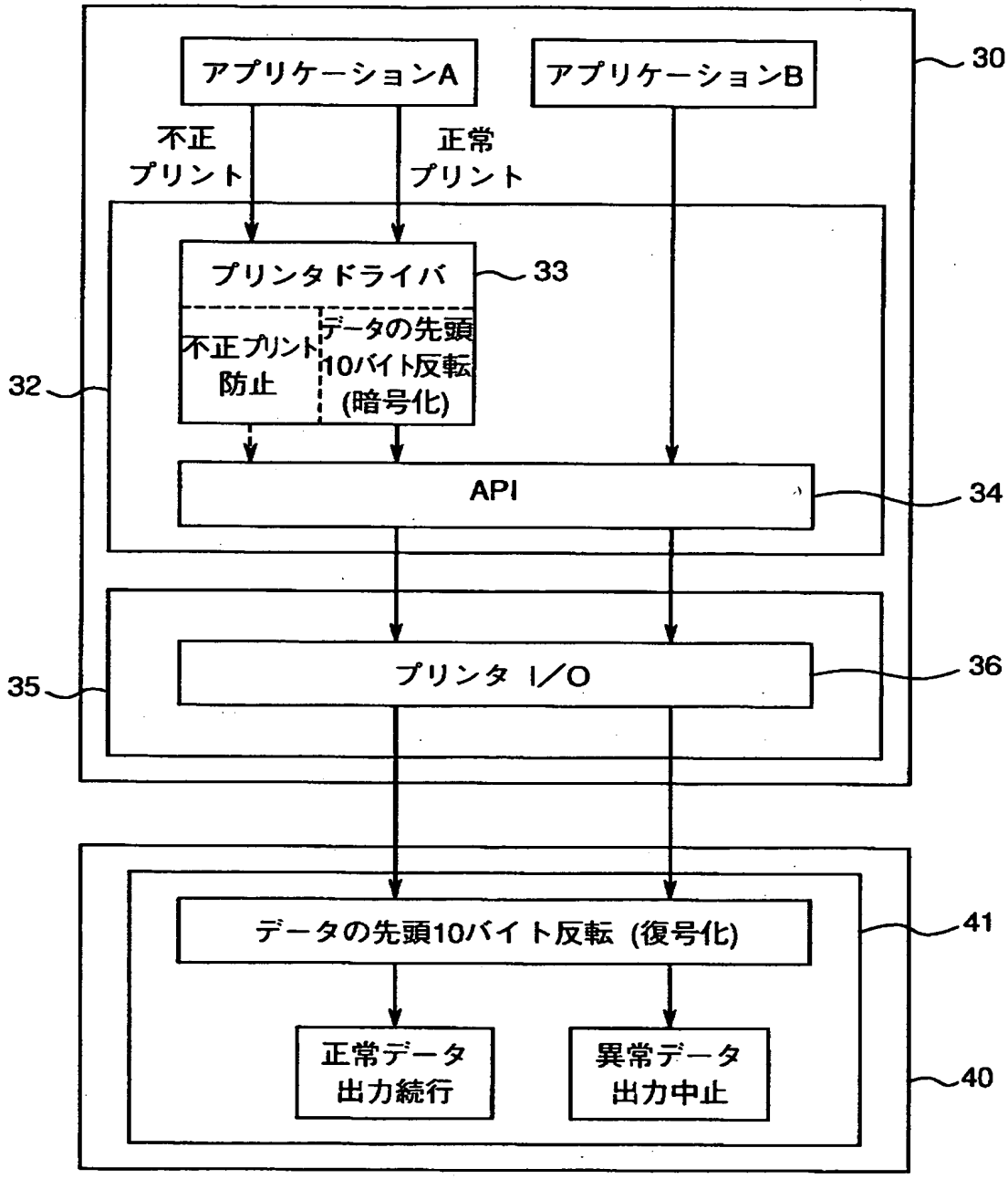
【図３】


スタート
#11
プリンタドライバ呼出し
#12
API呼出し
#13
APIコールをトラップする
#14
プリンタドライバを経由するデータか?
NO
YES
#16
プリンタドライバの不正プリント防止機能呼出し
#17
不正プリントか?
YES
NO
#18
プリンタへのアクセス拒否
#19
プリンタへアクセス
#15
プリンタへ直接アクセス禁止
#20
プリント出力
リターン

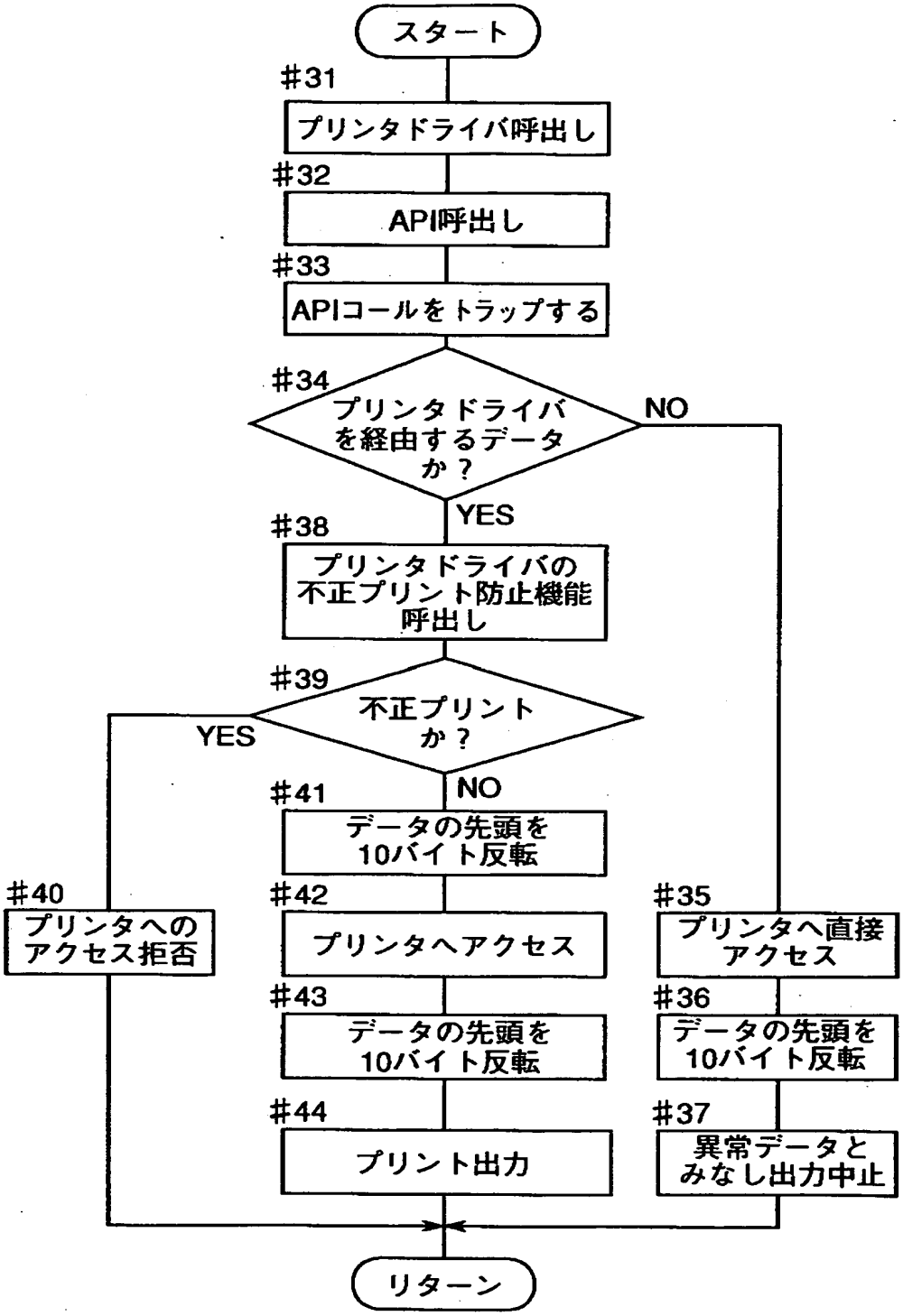
【図４】



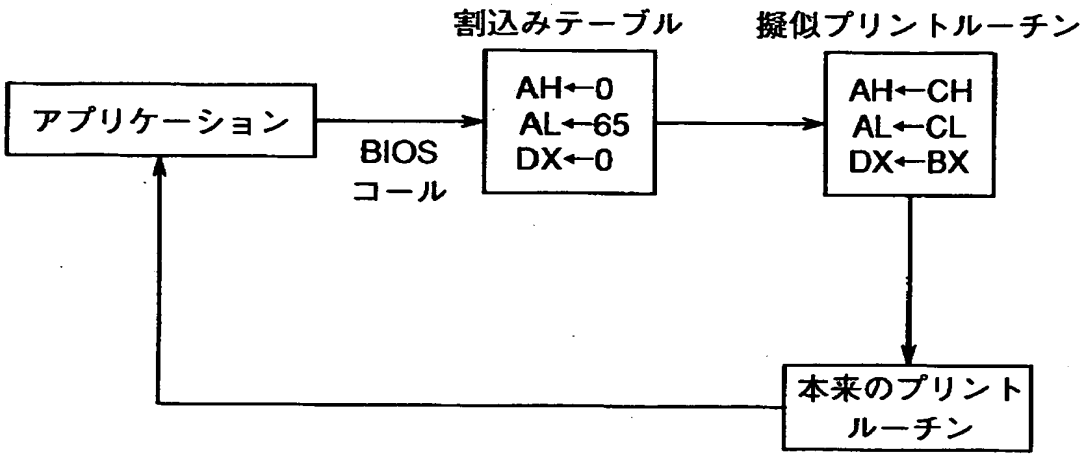
【図５】


アプリケーションA
アプリケーションB
30
不正
プリント
正常
プリント
プリンタドライバ
33
不正プリント
防止
データの先頭
10バイト反転
(暗号化)
32
API
34
プリンタ I/O
35
36
データの先頭10バイト反転 (復号化)
41
正常データ
出力続行
異常データ
出力中止
40

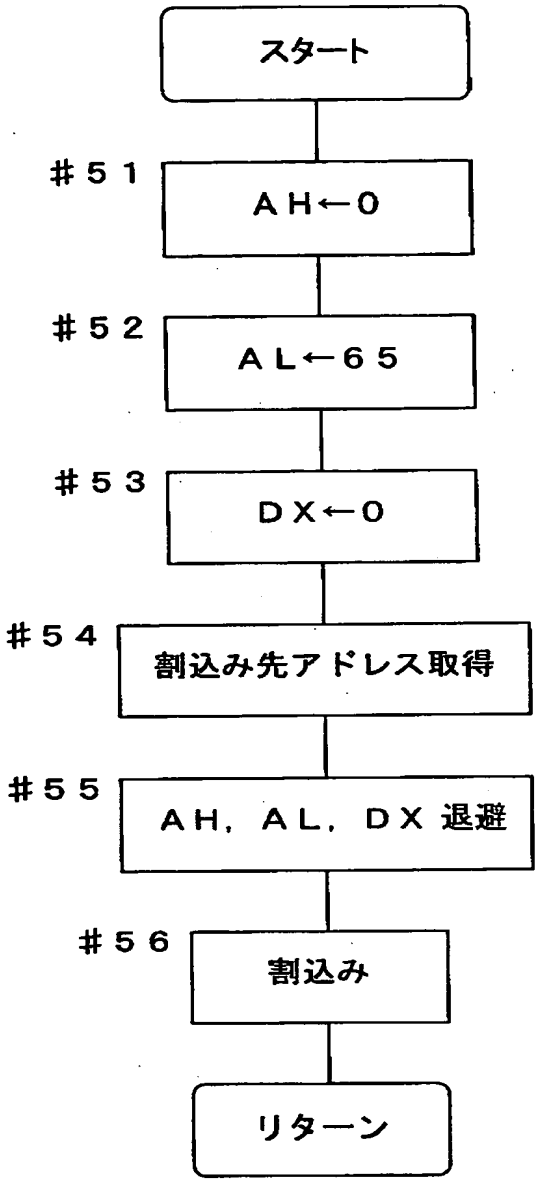
【図６】


スタート
#31
プリンタドライバ呼出し
#32
API呼出し
#33
APIコールをトラップする
#34
プリンタドライバを経由するデータか？
NO
YES
#38
プリンタドライバの不正プリント防止機能呼出し
#39
不正プリントか？
YES
NO
#41
データの先頭を10バイト反転
#40
プリンタへのアクセス拒否
#42
プリンタへアクセス
#35
プリンタへ直接アクセス
#43
データの先頭を10バイト反転
#36
データの先頭を10バイト反転
#44
プリント出力
#37
異常データとみなし出力中止
リターン

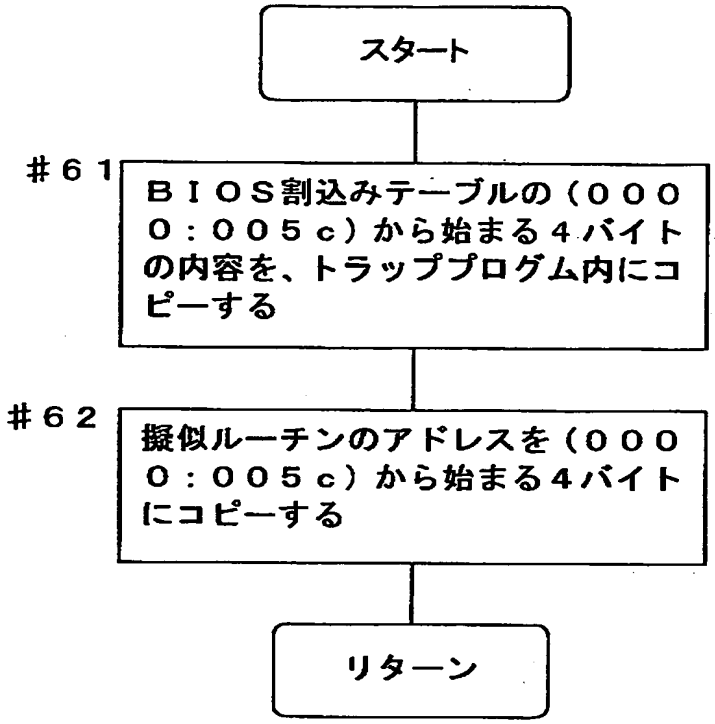
【図７】


割込みテーブル
擬似プリントルーチン
アプリケーション
BIOS
コール
AH←0
AL←65
DX←0
AH←CH
AL←CL
DX←BX
本来のプリント
ルーチン

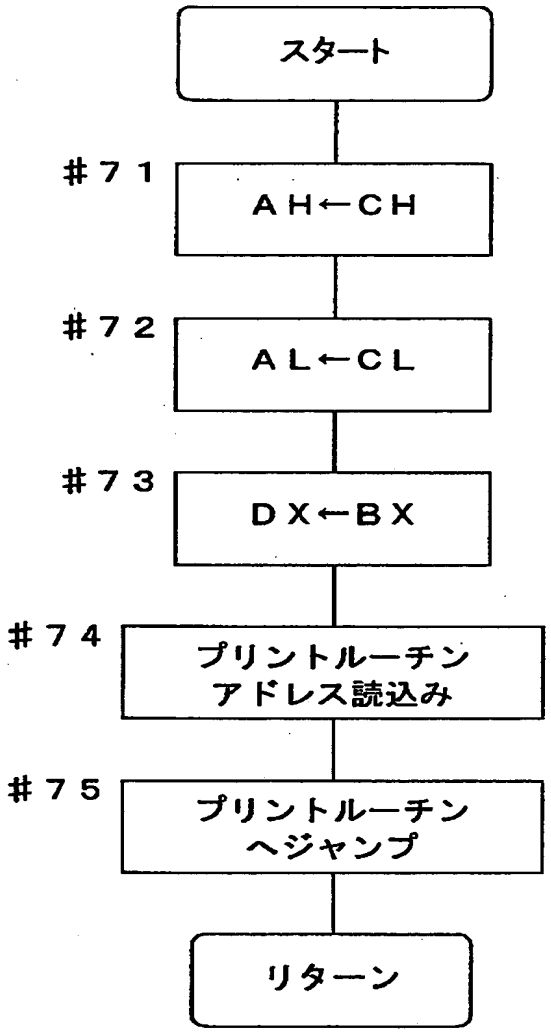
【図８】


スタート
＃５１
ＡＨ←０
＃５２
ＡＬ←６５
＃５３
ＤＸ←０
＃５４
割込み先アドレス取得
＃５５
ＡＨ，ＡＬ，ＤＸ 退避
＃５６
割込み
リターン

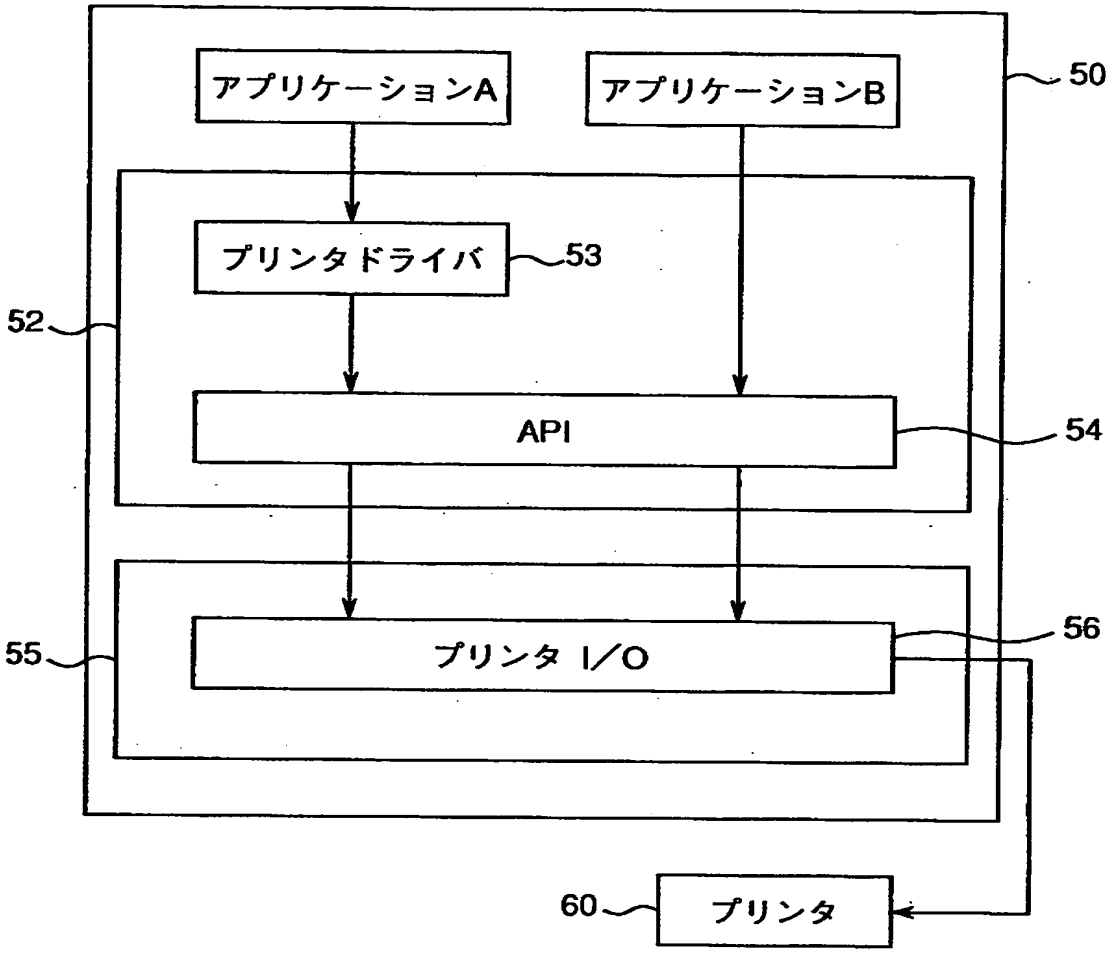
【図９】


スタート
＃６１
ＢＩＯＳ割込みテーブルの（００００：００５ｃ）から始まる４バイトの内容を、トラッププログム内にコピーする
＃６２
擬似ルーチンのアドレスを（００００：００５ｃ）から始まる４バイトにコピーする
リターン

【図１０】


スタート
＃７１
ＡＨ←ＣＨ
＃７２
ＡＬ←ＣＬ
＃７３
ＤＸ←ＢＸ
＃７４
プリントルーチン
アドレス読込み
＃７５
プリントルーチン
へジャンプ
リターン

【図１１】


アプリケーションA
アプリケーションB
50
プリンタドライバ
53
52
API
54
55
プリンタ I/O
56
60
プリンタ

【書類名】　要約書

【要約】

【課題】　安価且つ安全な出力システム及びそれに用いる出力方法並びに出力システムにおいて実行されるプログラムを記録した記録媒体を提供する。

【解決手段】　データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ送信に際し、上記ドライバソフトウェアを経由する出力要求であるか否かを判断した上で、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止する。

【選択図】　図３

# 出　願　人　履　歴　情　報

識別番号　　〔０００００６０７９〕

１．変更年月日　　１９９４年　７月２０日
［変更理由］　名称変更
住　所　　大阪府大阪市中央区安土町二丁目３番１３号　大阪国際ビル
氏　名　　ミノルタ株式会社